Los expertos en ciberseguridad han descubierto fallos de diseño en las funciones Windows Smart App Control y SmartScreen de Microsoft que podrían permitir a los atacantes obtener acceso inicial a sistemas objetivo sin activar alertas de seguridad.

Smart App Control (SAC) es una característica de seguridad basada en la nube lanzada por Microsoft en Windows 11 para bloquear aplicaciones maliciosas, no confiables y potencialmente no deseadas. Cuando el servicio no puede determinar la seguridad de una aplicación, verifica si está firmada o tiene una firma válida para permitir su ejecución.

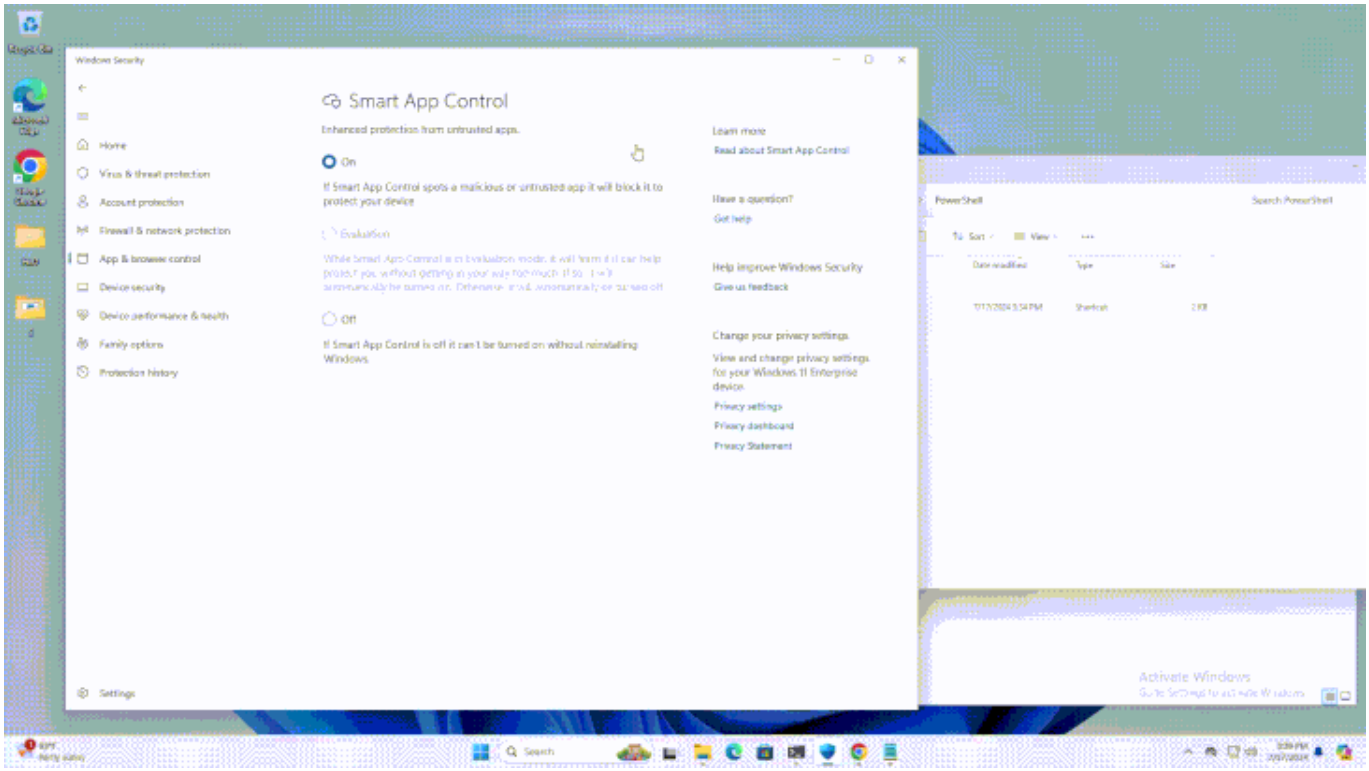
SmartScreen, que se introdujo con Windows 10, es una característica de seguridad similar que evalúa si un sitio web o una aplicación descargada podría ser peligrosa. También emplea un enfoque basado en la reputación para proteger URLs y aplicaciones.

> *«Microsoft Defender SmartScreen evalúa las URLs de un sitio web para determinar si se conocen por distribuir o alojar contenido inseguro,»* según la documentación de Redmond.
>
> *«También realiza comprobaciones de reputación para aplicaciones, revisando los programas descargados y la firma digital utilizada para firmar un archivo. Si una URL, un archivo, una aplicación o un certificado tiene una reputación establecida, los usuarios no reciben advertencias. Si no hay reputación, el elemento se marca como de mayor riesgo y presenta una advertencia al usuario.»*

También cabe mencionar que, cuando SAC está activado, reemplaza y desactiva Defender SmartScreen.

> *«Smart App Control y SmartScreen presentan una serie de debilidades de diseño que pueden permitir el acceso inicial sin alertas de seguridad y con mínima interacción del usuario,»* afirmó Elastic Security Labs en un informe.

Una de las formas más simples de eludir estas protecciones es obtener la firma de la aplicación con un certificado de Validación Extendida (EV), una táctica ya utilizada por actores maliciosos para distribuir malware, como se demostró recientemente en el caso de HotPage.



Algunos otros métodos que se pueden utilizar para evadir la detección son:

- Secuestro de Reputación: Consiste en identificar y reutilizar aplicaciones con buena reputación para sortear el sistema (por ejemplo, JamPlus o un intérprete conocido de AutoHotkey).
- Siembra de Reputación: Utiliza un binario aparentemente inofensivo controlado por el atacante para activar comportamientos maliciosos debido a una vulnerabilidad en una aplicación o tras cierto tiempo.
- Manipulación de Reputación: Modifica ciertas partes de un binario legítimo (por

ejemplo, una calculadora) para inyectar código sin perder su reputación general.

- LNK Stomping: Aprovecha un error en la forma en que Windows maneja los archivos de acceso directo (LNK) para eliminar la etiqueta de marca de la web (MotW) y sortear las protecciones de SAC, dado que SAC bloquea archivos con esa etiqueta.

> *«Esto implica crear archivos LNK con rutas de destino o estructuras internas no estándar. Cuando se hace clic en estos archivos LNK, son modificados por explorer.exe con el formato canónico. Esta modificación elimina la etiqueta MotW antes de que se realicen las comprobaciones de seguridad»,* indicaron los investigadores.

> *«Los sistemas de protección basados en la reputación son una capa eficaz para bloquear malware común. Sin embargo, al igual que cualquier técnica de protección, tienen debilidades que pueden ser eludidas con cierta atención. Los equipos de seguridad deben examinar detenidamente las descargas en su sistema de detección y no depender exclusivamente de las funciones de seguridad del sistema operativo para protegerse en este ámbito»,* comentó la empresa.